EUROSMART
The Voice of the Digital Security Industry

Position paper on proposed amendments on Artificial Intelligence Act

Four key principles to better oversee the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement

Some amendments of the IMCO/LIBE draft report on [AI Act] [1] may have very substantial impacts on the deployment and uptake of remote biometric identification systems while some other would lead to completely ban any 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement in Europe. Eurosmart would like to provide its analysis on the consequences of such amendments.

Amendments 1233, 1234, 1237 and 1244 would lead to completely ban any 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement in Europe. Eurosmart considers that the approach proposed by the European Commission in its proposal [AI Act] is balanced as it prohibits in principle the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, except for three well identified objectives. **This approach drastically limits the risks of mass surveillance and violations of personal freedoms while still allowing benefiting from these systems in some well identified situations (article 5(1)d). In that regard, Eurosmart recommends rejecting amendments 1233, 1234, 1237 and 1244.**

Regarding the definition of remote biometric identification systems, **Eurosmart recommends rejecting amendments 1053, 1054, 1055, 1056, 1057, and 1058** which considerably expand the scope of application of the text (1) to systems not only used for the purpose of identifying individuals using their biometry but also taking into account those only capable to do so, and (2) to facilitation usages (for which the individual has expressed its consent) that would be considered as high risk AI systems. As a conclusion expanding the scope of application of the text would further hinder the use of remote biometric identification systems. **Conversely, Eurosmart recommends retaining amendment 1059 which brings clarity with regards to facilitation usages**. **Also, Eurosmart recommends retaining amendments 1050, 1051 and 1052** which make a clear distinction between biometric identification system and biometric authentication system.

However, Eurosmart understands and fully shares the concern which underpins the proposed amendments 1233, 1234, 1237, and 1244 whereby 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement may be used to set up mass

[1] https://www.europarl.europa.eu/doceo/document/CJ40-AM-732837_EN.pdf
https://www.europarl.europa.eu/doceo/document/CJ40-AM-732838_EN.pdf

surveillance and violate personal freedoms of citizen, ultimately leading to weakening or even annihilating democracy in Europe. This concern is reinforced by foreign examples where these systems are used countrywide for mass surveillance and so called "social scoring". Therefore Eurosmart would like to propose four key principles to be introduced in [AI Act] to better oversee the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement.

The three exceptions for the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be maintained

Eurosmart believes that entirely banning 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is not the right approach for the following reasons:

- European Union is founded on democratic values. It ensures that rule of law is applied and guaranteed in each Member State. **Member States are deeply rooted in the democratic principles of the European Union : strong counter powers exist and independent justice allows citizen to contest decisions if they are not lawful. Therefore, the likelihood that these systems are diverted from their original lawful purpose for mass surveillance or control of individuals is very low**;
- **While these systems are used in non-democratic countries to carry out mass surveillance and control of individuals, it does not mean that such systems necessarily entails mass surveillance and violation of personal freedoms**. **Other kind of systems used in non-democratic regimes to carry out mass surveillance and violation of personal freedoms have been used for years in Europe in full compliance with fundamental rights and data protection requirements and it has not raised such debates**, such as :
    - Search Engines which logs the IP address and research of each individuals;
    - Mobile phone manufacturer or mobile app developer that can geolocate an individual;
    - Personal electronic devices (including mobile phones) manufacturer that can potentially identify user thanks to their behavior (habits, way to type, location...);

  In addition; these systems are usually operated by non-EU private stakeholders ruled by non-EU laws, which raises even more risks than the current situation where the 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement would be operated by entities ruled by EU laws, with proper checks and balances.

- **The focus and concerns from many stakeholders around these systems is surprising. In contrast, similar systems allowing identification in real time of individuals with a high level of confidence and relying on artificial intelligence do not raise such concerns**. For instance, this is the case for systems allowing identification of individuals thanks to the way they use their mobile phones (habits, way to type, location, cookies...). These systems use artificial intelligence in real time to identify individuals by exploiting the traces of their interaction with their mobile phones. Besides, as stated above, these systems are usually operated by non-EU private stakeholders ruled by non-EU laws. **Therefore it seems that the strong opposition to 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement rather appears as a firm opposition to biometric identification technology**. It may stem from the fear of individuals of being recognized by their face, which may create stress and thus may be perceived

as less acceptable. As such biometric identification is a bare technology, and as such is amoral: neither good nor bad. Technology can't be held responsible of its usage. Other technologies may also entail risks, yet they bring substantial benefits to humankind, i.e. chemistry, nuclear, genetic, computer vision that overpass the latter. Last but not least, **from a philosophical perspective, banning technologies is very disturbing, as this may constitute a very dangerous precedent**. **Over centuries, humankind has always innovated and developed new technologies, which brought prosperity, wealth and welfare. These latter are the ferment of the democracy, as democracy only exists where there is wealth to share. Without prosperity and wealth, and thus without innovation and new technologies, democracy is also at risk**. **Therefore, the legislator shall be very cautious when deciding to ban a specific technology as a pretext for preventing from mass surveillance or violation of personal freedoms, as it may in return put the democracy at risk.**

- **These systems are very useful** and bring substantial benefits to society to fight criminality or secure large events. **They could help transforming law enforcement by increasing the efficiency of police forces and strengthening citizen trust**. The use of biometric identification for criminal investigations has already brought outstanding results in the past. For instance, in France, it was instrumental to solve cold cases where innocent had been convicted or to establish 138 000 reconciliations of profiles which solved cases[2]. Interpol also declared that by the end of 2016, facial biometry helped identifying 1500 individuals[3] (terrorists, criminals, fugitives, persons of interest or missing persons). In addition, while large events are getting more and more popular and widespread, and the risks of terrorism or violence remain or even increase, these systems are the right counterpart ensuring these events could securely take place.

Therefore Eurosmart believes the current approach proposed by European Commission in [AI Act] enacted in article 5(1)d shall be kept as is, where the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is prohibited in principle, except for three well identified objectives. Eurosmart recommends that the proposed amendments 1233, 1234, 1237 and 1244 be rejected.

Definition of remote biometric identification system

The [AI Act] introduces in article 3(36) a definition of remote biometric identification system.

Amendments 1054 and 1055 propose to change the definition of remote biometric identification system in a very substantial manner. While the initial text in [AI Act] defines it as an AI system used for the purpose of identifying natural persons using biometric technology, these amendments propose to change it to an AI system capable of identifying natural persons. Pursuant to these amendments, the very nature of an AI system – and not its purpose - would be sufficient to classify it as a remote biometric identification system**. It would entail that an AI system which is simply capable of identifying natural persons using biometry, but that does not use this capability would fall into this modified definition, and thus would be considered as a high risk AI system (pursuant to Annex III)**. Today, for instance some smartphones or operating system for computers implement facial or iris identification, which means that they would fall into this new definition of remote biometric identification system. As the software is not considered as a product, **nearly all devices (computer, smartphone...) would fall into this updated definition of remote biometric identification system and thus would become high risk AI system (pursuant to Annex III)**. Instead of being absolute and

[2] Fichier national automatisé des empreintes génétiques — Wikipédia (wikipedia.org)
[3] Facial Recognition (interpol.int)

including all AI systems capable of identifying natural person with biometric technology at a distance, this definition should only consider AI systems which may entail substantial risks for user. It requires to consider the purpose of the AI system and not only its capacity. **Therefore Eurosmart recommends rejecting amendments 1054 and 1055.**

A remote biometric identification system as proposed in article 3(36) is defined by (1) its purpose and (2) the usage ("[…] and without prior knowledge of the user of the AI system whether the person will be present and can be identified"). The latter aims at excluding **facilitation usages** from the definition of remote biometric identification system, **whereby the individual's presence is expected by the user of the AI system, so that he can seamlessly access a resource, cross a point or go in an area. It allows individuals to move without having to stop at a check point, which substantially increase the person's experience, enhances security by allowing human expertise to focus on sensitive cases. This implies a previous registration, which means a cooperation, informed consent and consciousness from the individual. Typical examples are physical access control, border crossing in an airport or railway station, or securely opening a computer session with the right profile (e.g. Windows Hello which uses biometric identification as a computer may be shared across family members)**. Therefore, such usages are ruled by GDPR[4] and fall under the provisions of article 6(1)a for which the individual has given its consent. **Besides, as these usages represent no material risk to citizens' fundamental rights, it is normal that they are excluded from the definition of remote biometric identification system, and thus not considered as a high risk AI system (pursuant to Annex III)**. Last but not least, this exception also allows implementing facilitation usages carried out by a 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, such as (1) seamless border crossing at airport or in railway station or (2) seamless access to a restricted area, as they do not fall into the provisions of article 5(d)1. It is of the utmost importance to ensure that these usages are permitted as they are instrumental to streamline control and increase throughput especially where space is limited for having people queuing (e.g. airport), or police forces are not sufficient. **In that regards, Eurosmart recommends rejecting amendments 1053, 1054, 1055, 1056, 1057, and 1058 which propose to remove this exception. Besides, Eurosmart very much welcomes amendment 1059 which provides a better and clearer description of the exception at stake by introducing the notion of conscious cooperation.** This amendment proposes that the definition of a remote biometric identification system shall:

- exclude usages where the identified individual claims having a particular identity authorization, or accreditation, meaning usages for which the individual has previously registered and consented to;
- include usages where the identity of the identified individual is not established with his conscious cooperation, meaning the identified individual has not consented to be identified, thus potentially representing a potential harm to their fundamental rights;

Eurosmart considers this definition is very good and recommends amendment 1059 to be retained.

Eurosmart also welcomes amendments 1050, 1051 and 1052 which supplement the proposed definition of remote biometric identification system to clarify that such system does not include biometric system carrying out biometric authentication. These amendments reflect that biometric authentication has a very different nature from biometric identification. While biometric identification consists in identifying someone by searching in a database the individual matching the biometric data that has been captured, the biometric authentication simply consists in confirming than a biometric

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) - EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)

data matches the expected individual. It implies that the system knows ahead of time the individual to authenticate. **Eurosmart recommends retaining amendments 1050, 1051 and 1052.**

In addition Eurosmart welcomes amendment 1048 which supports the same objective as above. However Eurosmart believes that amendments 1050, 1051 and 1052 are much better as they address the topic in a more generic manner.

Four key principles to better oversee the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement

Eurosmart also acknowledges that the concern expressed by the proposed amendments 1233, 1234, 1237, and 1244 shall be heard and answered. **Therefore Eurosmart recommends that the proposed regulation be amended to strengthen the supervision and transparency of these systems in order to reinforce citizen trust. In particular, Eurosmart would like to suggest the following four principles that should be reflected in [AI Act] as amendments.**

1 Principle#1: Introduce transparency and accountability obligations for the entities operating a 'real-time' remote biometric identification system in publicly accessible spaces for the purpose of law enforcement falling under the provisions of article 5(d)1

- **The entity shall ensure that the systems comply with the recommendations prepared by European Data Protection Board (EDPB)** on the use of facial recognition technology in the area of law enforcement (Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement[5]);
- **The entity shall duly justify the proportionality of the technical features of the system with its needs and goals**. In particular, the sizing of the system - i.e. the maximum number of biometric data records in reference database the system should manage and process - shall be justified;
- **The entity shall provide the data governance model and description applicable to the biometric data records** in the reference database used by the system. It encompasses, but is not limited to, (1) the reasons for adding or removing a biometric data record from the reference database, (2) the qualification of the operators entitled to perform action on these biometric data records, or (3) the duration after which a biometric data record in the reference database shall be erased;
- **The log files generated by the systems shall be auditable and freely available to the national data or fundamental right protection authorities**.

[5] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en

2 Principle#2: 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement falling under the provisions of article 5(d)1 shall implement technical limitations not to be diverted from their original lawful purpose by the entities operating them in order to carry out mass surveillance or violation of personal freedoms

- **remote biometric identification systems shall be designed to manage and process a limited number of biometric data records in reference database**. This limit shall be commensurate with the sizing of the system as defined by the entity (see principle#1);
- **It shall not be possible for the entity to manage more biometric data records in reference database than the limit aforementioned**.

3 Principles#3: 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement falling under the provisions of article 5(d)1 shall be designed to support privacy, transparency and accountability

- The system shall ensure privacy by design;
- Each addition or removal of biometric record in reference database shall require (1) identification and strong authentication of the operator and (2) the provision of the reason for such operation;
- Each addition or removal of biometric record in reference database shall be automatically recorded in log files (date, reasons, identification of the operator…);
- The system shall ensure that each record in the log file is non-repudiable;
- The system shall ensure that the content of log files is human readable so that it could be easily audited;
- The system shall ensure that it is not possible to erase, modify or tamper with the content of the log files;

The system shall ensure a retention duration for log files of at least 12 months. This duration is in line with the proposed obligation for Member States to submit an activity report to the European Union Artificial Intelligence Board each year.

4 Principle#4: Organise an efficient European supervision of 'real-time' remote biometric identification systems in publicly

- **Before a system is set up, the Member State shall notify the European Commission and shall communicate the conformity assessment of such system with the European Data Protection Board (EDPB) recommendations (see principle#1);**
- The Member State shall notify the European Commission of:
  1. **the conformity assessment of the system with the EDPB recommendations**;
  2. **the justification of the proportionality of the technical features of the system with the authority needs and goals**;
  3. **the data governance model and description applicable to the biometric data records**
  4. **the limit of biometric records the system can handle and process**;

The Member State shall also notify the European Commission where there is a change or upgrade which significantly alters the capabilities of the system, typically in terms of size of the reference database or volume of data processed by the system.

- Each year, the Member State shall submit an activity report to the European Union Artificial Intelligence Board;
- The notifications and activity reports submitted by Member States shall be reviewed by the European Union Artificial Intelligence Board, which shall issue an opinion. The European Commission, based on the opinion of the European Union Artificial Intelligence Board , shall conclude on whether a deployed 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement falling under article 5(1)d complies with the EU laws;

References

[AI Act] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) ND AMENDING CERTAIN UNION LEGISLATIVE ACTS (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206)